


Form PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE (REV 10-95)		ATTORNEY'S DOCKET NUMBER 1376-010862
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. 097856813 <small>(If known, enter Class.)</small>
INTERNATIONAL APPLICATION NO PCT/AU99/01051	INTERNATIONAL FILING DATE 25.11.99 (November 25, 1999)	PRIORITY DATES CLAIMED 25.11.98 (November 25, 1998)
TITLE OF INVENTION HIGH ASSURANCE DIGITAL SIGNATURES		
APPLICANT(S) FOR DO/EO/US John Desborough YESBURG		
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:		
<p>1. <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.</p> <p>2. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.</p> <p>3. <input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).</p> <p>4. <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.</p> <p>5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2))</p> <p>a. <input type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau)</p> <p>b. <input checked="" type="checkbox"/> has been transmitted by the International Bureau</p> <p>c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US)</p> <p>6. <input type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)).</p> <p>7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))</p> <p>a. <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau)</p> <p>b. <input type="checkbox"/> have been transmitted by the International Bureau</p> <p>c. <input type="checkbox"/> have not been made, however, the time limit for making such amendments has NOT expired</p> <p>d. <input checked="" type="checkbox"/> have not been made and will not be made.</p> <p>8. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3))</p> <p>9. <input type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))</p> <p>10. <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5))</p> <p>Items 11. to 16. below concern document(s) or information included:</p> <p>11. <input type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98</p> <p>12. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.</p> <p>13. <input checked="" type="checkbox"/> A FIRST preliminary amendment</p> <p><input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment</p> <p>14. <input type="checkbox"/> A substitute specification.</p> <p>15. <input type="checkbox"/> A change of power of attorney and/or address letter</p> <p>16. <input checked="" type="checkbox"/> Other items or information:</p> <p>a. WO 00/31644-Front Page with Abstract, Specification, Claims, Drawings and Search Report (48 pp.)</p>		

U.S. APPLICATION NO. 09/856813		INTERNATIONAL APPLICATION NO. PCT/AU99/01051		ATTORNEY'S DOCKET NUMBER 1376-010862	
17. <input checked="" type="checkbox"/> The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO \$860.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) \$690.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) \$710.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$1,000.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$100.00				CALCULATIONS PTO USE ONLY	
ENTER APPROPRIATE BASIC FEE AMOUNT =				\$ 860.00	
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input checked="" type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$ 130.00	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	23 - 20	3	X \$18.00	\$ 54.00	
Independent claims	1 - 3 =	0	X \$80.00	\$ 0.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$270.00	\$ 0.00	
TOTAL OF ABOVE CALCULATIONS =				\$ 1,044.00	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28)				\$ 0.00	
SUBTOTAL =				\$ 1,044.00	
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f))				\$ 0.00	
TOTAL NATIONAL FEE =				\$ 1,044.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)) The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) \$40.00 per property				\$ 0.00	
TOTAL FEES ENCLOSED =				\$ 1,044.00	
				Amount to be: refunded	\$
				charged	\$
a. <input checked="" type="checkbox"/> A check in the amount of \$1,044.00 to cover the above fees is enclosed b. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees A duplicate copy of this sheet is enclosed c. <input checked="" type="checkbox"/> The Assistant Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>23-0650</u> . A duplicate copy of this sheet is enclosed NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.					
SEND ALL CORRESPONDENCE TO Richard L. Byrne 700 Koppers Building 436 Seventh Avenue Pittsburgh, Pennsylvania 15219-1818 Telephone: (412) 471-8815 Facsimile: (412) 471-4094					
				SIGNATURE <u>Richard L. Byrne</u> NAME 28.498 REGISTRATION NUMBER	

09/856813

JC18 Rec'd PCT/PTO 2 5 MAY 2001

PATENT APPLICATION/PCT
Attorney Docket No. 1376-010862

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
John Desborough YESBURG : **HIGH ASSURANCE DIGITAL**
: **SIGNATURES**
International Application :
No. PCT/AU99/01051 :
International Filing Date :
25 November 1999 :
Priority Date Claimed :
25 November 1998 :
Serial No. Not Yet Assigned :
Filed Concurrently Herewith :

Pittsburgh, Pennsylvania
May 25, 2001

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, DC 20231

Sir:

Prior to initial examination, please amend the above-identified patent application
as follows:

IN THE SPECIFICATION:

Please insert and amend section headings as follows:

On page 1, after the title, please insert the following section headings:

BACKGROUND OF THE INVENTION

1) Field of the Invention

**On page 1, please amend the section heading "Background" to read as
follows:**

2) Description of the Prior Art

On page 10, after the second complete paragraph, please amend the section heading "BRIEF DESCRIPTION OF THE INVENTION" to read as follows:

SUMMARY OF THE INVENTION

IN THE CLAIMS:

Please cancel the previous versions of claims 3, 15-19, 21 and 22 and insert the amended versions of claims 3, 15-19, 21 and 22 as follows. (Pursuant to 37 CFR 1.121, marked-up versions of these claims are attached.)

3. (Amended) A private key protection system according to claim 1, wherein said signed digital data is a digital certificate.

15. (Amended) A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines how said encryption engine should encrypt or decrypt respectively.

16. (Amended) A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines which protocol is used by said device to communicate encrypted or signed data external of said device.

17. (Amended) A digital private key protection device according to claim 1, wherein said display means is external to said device and controlled by said device for displaying data transmitted from said communications port.

18. (Amended) A digital private key protection device according to claim 1, wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner.

19. (Amended) A digital private key protection device according to claim 1, further comprising identification and authentication means actuated by said user in a predetermined manner.

21. (Amended) A digital private key protection device according to claim 1, wherein said digital private key storage means is removable from said device.

22. (Amended) A digital private key protection device according to claim 1, wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said PKPD using the user's private or other keys as identified by the request, but excluding the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.

IN THE ABSTRACT:

After the claims, please insert a page containing the Abstract Of The Disclosure, which is attached hereto as a separately typed page.

REMARKS

Amendments have been made to the specification in order to conform the specification to standard United States Patent practice.

Original claims 3, 15-19, 21 and 22 have been amended to eliminate the multiple dependencies and to conform the claims to standard United States practice.

An Abstract Of The Disclosure has been added as a separately typed page to be inserted after the claims.

Examination and allowance of claims 1-23 are respectfully requested.

Respectfully submitted,

WEBB ZIESENHEIM LOGSDON
ORKIN & HANSON, P.C.

By 

Richard L. Byrne, Reg. No. 28,498
Attorney for Applicant
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219-1818
Telephone: 412/471-8815
Facsimile: 412/471-4094

MARKED-UP AMENDED SECTION HEADINGS

Page 1, section heading

[Background] 2) Description of the Prior Art

Page 10, section heading

[BRIEF DESCRIPTION OF THE INVENTION] SUMMARY OF THE INVENTION

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2

MARKED-UP AMENDED CLAIMS

3. (Amended) A private key protection system according to [claims 1 and 2] claim 1, wherein said signed digital data is a digital certificate.

15. (Amended) A digital private key protection device according to [any preceding claim] claim 1, wherein said received digital data contains an instruction which determines how said encryption engine should encrypt or decrypt respectively.

16. (Amended) A digital private key protection device according to [any preceding claim] claim 1, wherein said received digital data contains an instruction which determines which protocol is used by said device to communicate encrypted or signed data external of said device.

17. (Amended) A digital private key protection device according to [any preceding claim] claim 1, wherein said display means is external to said device and controlled by said device for displaying data transmitted from said communications port.

18. (Amended) A digital private key protection device according to [any preceding claim] claim 1, wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner.

19. (Amended) A digital private key protection device according to [any preceding claim] claim 1, further comprising identification and authentication means actuated by said user in a predetermined manner.

21. (Amended) A digital private key protection device according to [any preceding claim] claim 1, wherein said digital private key storage means is removable from said device.

22. (Amended) A digital private key protection device according to [any preceding claim] claim 1, wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said PKPD using the user's private or other keys as identified by the request, but excluding the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228

HIGH ASSURANCE DIGITAL SIGNATURES

ABSTRACT OF THE DISCLOSURE

A digital private key storage means containing a user's digital private key; a cryptographic engine; a communications port for receiving digital data from an external device, and for transmitting data to said external device; a display means for displaying said received digital data; a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data; wherein said cryptographic engine is trusted to only apply said user's digital private key to sign received data only if said user operable input means is operated, and to communicate said signed data external of said digital private key protection device. This arrangement secures the user's digital private key from end point attacks by trojan horse programs by virtue of the fact that the private key can only be accessed via the user operable input means which cannot be circumvented by software control.

HIGH ASSURANCE DIGITAL SIGNATURES

This invention relates to digital signatures and in particular to high assurance digital signatures.

Background

Signatures are used by people in all aspects of everyday life. As society moves inexorably into the age of computers and information technology, the need for a signature which can be used in the digital realm is rapidly becoming a necessity.

Digital signatures however are not new and have been described in the research literature for nearly 20 years, but are not yet capable of being described as "commonplace".

However, as more security critical information is exchanged digitally, and more importantly the economic value of the information and transactions being handled digitally becomes more important, the need for a secure digital signature is likewise increasing in importance.

For the use of digital signatures to become readily accepted in high value or high-risk applications, it is necessary for them to be secure and there are a number of aspects to this security which are necessary precursors to their commonplace use in the future:

1. The cryptographic algorithms used to generate signatures have to be complex enough to be unbreakable;

2. The users of the system need to have confidence in the public key distribution infrastructure;
3. The storage of private keys needs to be secure; and
4. The "endpoint" at which encryption is performed and signatures are created or validated needs to be secure.

The literature describes numerous successful attacks against security measures taken to ensure the abovediscussed issues.

The invention described herein relates in particular to the fourth aspect of the security issues mentioned above, by providing a secure "endpoint" for encryption and the creation and validation of digital signatures.

Endpoint attacks

Endpoint attacks affect the act of encryption and the creation or validation of digital signature, consequently the possibility of Endpoint attacks lower the confidence of the recipient of a digital messages that the message has been properly signed. The recipient may be unsure as to whether the digital message is original or indeed originates from the purported sender of the message.

An endpoint attack is different to a "protocol" attack which typically occurs during the transit of the message. In an endpoint attack, the attacker typically alters software on a sender's computer, so that the altered software modifies one or more messages which are being sent and received or initiates the sending of messages without the knowledge of the sender. Whereas in a protocol attack, an attacker eavesdrops on communications between the respective computers of the

sender and receiver and can impersonate either of the participants, or modify missives, etc.

There exist encryption techniques which can reduce or eliminate protocol attacks. However, endpoint attacks in the critical area between the user and their own computer are not aided by the encryption approach.

High assurance security and Endpoint attacks

Technology for building secure systems has mostly been developed in the military intelligence communities. In high-risk situations, policies require high assurance systems. That is, the users or owners of systems have to be highly assured, or confident, that the software and hardware systems they use will perform correctly. The consequences of failure can be so significant, that it is justifiable to spend substantial amounts of time and effort to achieve this assurance.

Assurance of this type is aimed partly at countering the threat of endpoint attacks and such assurance can be gained in a number of ways.

The most rigorous and objective methods, used by military and intelligence organisations, are described in publications such as TCSEC, ITSEC, and CC which provide a variety of physical, procedural and hardware and software approaches which for this specialist environment can provide the necessary assurances.

However, the majority of computers and computer systems used in critical environments do not meet the high levels of assurance which might be required by policy.

History has shown that the procurement of suitably secure and assured general purpose computer systems is very expensive and impractical. They are typically obsolete before they are delivered.

A device which provides high assurance digital signatures used as a limited-functionality peripheral provides a means for achieving high assurance security functions without the disadvantages associated with the development and evaluation of a much more complex, general purpose computer system.

Digital signature semantics

Signatures in the "paper" world (in contrast to the purely "digital" world) are used to indicate that the person who signs the document has written or read and thereby agrees with the content of the document and in accordance with its content, is bound by the fact of the signature to abide by that content. The term signature can also include the mark of a legal entity which may be represented in the form of a company seal applied by an authorised officer of the legal entity and typically countersigned by that person. Documents requiring signatures include, but are not restricted to, personal letters, contracts, or cheques.

Although there are many (surprisingly simple) ways to forge a signature, or undetectably modify the document which was signed, in critical circumstances there do exist well accepted procedures to increase the assurance that a signature has been applied by the appropriate person and that they were not under any duress at the time (eg witnesses).

Thus it is desirable that, when digital signatures are used for the purpose of positively identifying the person who applied the digital signature, the signed

digital message/ document has the same legal value and effect as signatures used on a paper document.

As with paper documents, if a digital document is signed by a person or a legal entity, the recipient and reader of the document should be able to safely assume that the signer has written or at least read and agrees with the content of the document.

However, in a digital world it is even easier than in the paper world to change documents without detection, least likely but most importantly the creator of the (unsigned) document.

In the digital world attacks occur almost instantaneously and in a realm not physically examinable by its users, attacks can originate from those very same devices that users grow to rely on, "their own computer" and in a manner which can leave little, if any, no evidence of the mechanism or the attacker. Thus in the current digital world it is prudent not to place too much reliance on the veracity of a digitally signed message or document

Assumed threats

There are many computer systems today which can generate digital signatures for use with documents but they are all still vulnerable to "endpoint" attacks. The designers and users of digital signing programs are often unaware of this type of threat and for those that are aware, the confidence or trust that a recipient can place in the fact that a statement was signed is never high and potentially the whole system of digital signature and certificates will be placed into jeopardy if this threat is not properly addressed. This jeopardy increases as time passes by,

and becomes more critical as more and more users are seduced by the apparent surety of the current system.

One manifestation of a real and active endpoint threat is exemplified by the "Trojan horse" type attack. A Trojan horse is malicious software, of which a user of the computer is typically unaware or of when and how it operates. The Trojan horse software, as the name suggests, gains access to the memory of the computer being used, by (surreptitiously) accompanying the loading of a legitimate software program and once ensconced inside the computer, performs malicious functions, without the knowledge of the user.

It is advantageous to provide some explanation of the terms which will be often used in the description of the technology surrounding and defining the invention.

Public Key Cryptosystems (also known as Asymmetric Cryptosystems)

This is a well known art, described in many references.

In standard (symmetric, or secret key cryptosystems), the encryption and decryption operations use the same key. However, in public key cryptosystems, one key is used for encryption, and the decryption can only be performed with a certain other key. The two keys are related, and sometimes called a key pair. One key is usually designated a "public" key and the other a "private" key. The security of the system relies on the fact that it is computationally infeasible to derive that private key given the public key.

It is generally assumed that any participant in information exchanged can acquire a user's public key, but that the user will protect the private key to the best of their ability.

If the public key is used to encrypt some information, only the holder of the private key will be able to decrypt the information. This is useful for encrypting messages destined for a particular user, which should not be disclosed to any other user. If the private key is used to encrypt some information, any user will be able to decrypt the information with the public key. This will assure other users that it was only the holder of the private key who actually encrypted the message originally. This is useful for implementing a digital signature which comprises the transformation of the message using the private key to produce a string of digital data which uniquely represents the message and from which it is infeasible to decrypt the original message. Only the other of the key pair, in this case the corresponding public key, can determine whether the original document was used to create the signature. Furthermore, it is also possible to encrypt a message with a public key which can only be decrypted with the corresponding private key.

The use by a user of their private key is seen by most as the equivalent of physically signing the content of the message, as it is typically assumed that only the holder of the private key could encrypt it and only the public key could decrypt it. This also of course assumes that the public key verifiably corresponds to the private key.

For efficiency purposes, encryption of messages is frequently performed by using a symmetric algorithm (which is faster) to encrypt the message using a randomly generated message encryption key, then using the asymmetric algorithm to

encrypt the "message encryption key" with the recipient's public/private key. Only the recipient, with a corresponding public/private key, will be able to decrypt the "message encryption key", with which they can then decrypt the actual message.

Similarly, for signing a document, it is usual to calculate a "message digest" using a hash function. It is the digest (which is much shorter than the message) that is then encrypted with the signer's private key. This encrypted digest is called the signature. A recipient can decrypt the signature to recover the original digest value. The signature is valid if the hash of the message is equal to the decrypted signature.

Cryptographic Engine

A cryptographic engine is an electronic component which is able to perform the complex arithmetical and logical manipulations involving data and keys, to implement encryption, decryption, signature generation, and signature validation. A cryptographic engine may include a number of registers for storage of keys and/or intermediate results.

The designer of a cryptographic engine would typically expect that the engine would be used to perform various calculations in order to give senders and recipients various assurances about the confidentiality, integrity, or origin (or similar) of a message. This assurance can only be given if the engine operates correctly, even in the presence of certain threats (which the designer will typically be aware of). The engine should be trusted, for example, not to release unencrypted data when encrypted data is required.

Examples of cryptographic engines are the Capstone chip, a Fortezza Card, an encryption daughter board for a PC, and a software module in a program such as PGP.

Endpoint Attack

A typical endpoint attack may occur in the following manner.

Consider a user who wants to sign an e-mail message. The user's private key is typically stored in an encrypted state in a file on the hard disc of the user's personal computer. To create the signature, the user must enter a password or phrase which allows the file to be decrypted and the unencrypted private key temporarily stored in the computer so that the e-mail program can then perform the cryptographic calculations on the message to produce the signature using the private key.

The signature created is an upwards of 64 ASCII character length string which uniquely correlates the user's private key with the digital representations of the message.

Consider an endpoint attack which modifies the behaviour of the users e-mail program. It would be possible for the malicious program to read and then store the various keys used by the user (in particular the key strokes that comprise the pass word or phrase) in another location on the hard disc. Having knowledge of the pass phrase or a copy of the key/s allows the malicious program to sign other messages, which the user did not intend to sign. For example, messages authorising the purchase and shipping of goods to a unknown recipient could be created and signed, all without the authority or knowledge of the user. The Trojan horse program may also secretly communicate the private key or keys of

the user to another user, who could then fraudulently forge the user's digital signature onto any document supposedly sent by the original user.

This is the primary threat countered by the present invention.

This invention provides a means for securing against the unauthorised use of a user's private key which as a consequence provides high assurance that the digital signatures created by that key are legitimate. The invention can be embodied in a number of forms each of which is useful in different applications.

BRIEF DESCRIPTION OF THE INVENTION

In a broad form of the invention a private key protection device (PKPD), comprises a digital private key storage means containing a user's digital private key; a cryptographic engine; a communications port for receiving digital data from an external device, and for transmitting data to said external device; a display means for displaying said received digital data; a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data; wherein said cryptographic engine is trusted to only apply said user's digital private key to sign received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device.

Specific embodiments of the invention will now be described in some further detail with reference to and as illustrated in the accompanying figures. These embodiments are illustrative, and not meant to be restrictive of the scope of the invention. Suggestions and descriptions of other embodiments may be included but they may not be illustrated in the accompanying figures or alternatively

features of the invention may be shown in the figures but not described in the specification.

BRIEF DESCRIPTION OF THE FIGURES

Fig. 1 depicts a pictorial representation of elements of an embodiment of a private key protection device;

Fig. 2 depicts a further pictorial representation of elements of a further embodiment of a private key protection device;

Fig. 3 depicts the use of a message envelope created by the PKPD;

Fig. 4 depicts the use of a message envelope created by the PKPD;

Fig. 5 depicts the PKPD attached to a PC wherein the device has an in built display;

Fig. 6 depicts the PKPD attached to a PC wherein the device incorporates a keyboard, video and mouse pointer switching function; and

Fig. 7 depicts a network comprising devices attached to PC's in the network.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

When a user wishes to sign a document they created themselves or one that was received and has been amended, they use their private key which is typically stored on the hard drive of their personal computer PC. Their private key is in encrypted form so that not just anyone can locate it and use or copy it, so the

12

users will need to input a pass phrase known only to them to "unlock" use of the private key for the signing process.

As discussed previously, it is during the time the private key is "unlocked" that the PC and user are most vulnerable to an "endpoint" attack. Even if the key is contained in a supposedly more secure device, such as a smartcard or a PCMCIA card such as a Fortezza card, it will be apparent to the reader that malicious software will still be able to utilise the unprotected key or the cryptographic services of the device. As soon as the device is unlocked (by the user entering a PIN), the device will perform whatever calculations it is asked to perform, whether the user is aware of these or not.

The invention comprises a private key protection device (PKPD) which is capable of resisting "endpoint attacks" thus ensuring the safety of the private key at all times.

In its simplest embodiment the PKPD exists separate from the user's PC but connects to it and its peripherals as required via normal communication ports. The embodiment depicted in Fig. 1 shows the PKPD 10 receiving 12 and transmitting data 14 via a communications port 16 of a device 18 which could be a PC. In this embodiment the PKPD lies between the user 20 and the PC 18.

The PC can send any data to the PKPD, which may be for example a shopping order list, a military command to fire a missile, or a contract. The PKPD receives the data at its communications port 22 and directs the data to the display 24.

The display 24 displays to the user the data to be reviewed plus any other command or prompts required to enable the user to control the use of the "private key" which is stored in the private key storage means 26.

Once the user has read and understands the document displayed, if they do not agree or are not willing to authorise the meaning of its contents they can ignore it and the document will be removed by a reset of the PKPD or some such other approach which ensures that the document has been permanently removed from the PKPD.

If the user agrees with or authorises the contents of the document, just as they would in the paper domain, they can choose to digitally sign the document.

This is achieved using the PKPD by manually operating the user operable input means 28 which may be integrated with the PKPD. This input means may be labelled variously, an ACCEPT button, a SIGN button, etc and may have various mechanical properties. For example, it may be a momentary contact switch, it may be locked and unlocked for manual operation and inoperable without a physical key, it may be backlit when operable, it may require a predetermined depression sequence. These features are merely additional to the primary requirement of being user operable in the physical sense.

Once the user operable input means 28 is operated, the cryptographic engine 30 will access the user's private key in the private key storage means 26 and use it to generate a digital signature of the document and only that document which was displayed to the user.

Once the document is signed, it is transmitted to the PC 18 via the transmit data path 14 via both communications ports 22 and 16. A communications port is a device which transmits or receives digital data to/from another port using a common protocol. A communications port may comprise hardware (eg parallel "centronics" printer port RS232 protocol port) or a logical software arrangement (eg TCP/IP port). The transmission and reception of digital data could be conducted via wire or wireless means.

The electronic means to implement the above functions of the PKPD can be implemented by a person skilled in the art.

A PKPD counters endpoint attacks and assuming that the cryptographic algorithms are not breakable, and that there is confidence in the public key distribution infrastructure, it becomes possible to trust the use of private keys. It becomes accepted that the person purported to have applied the signature actually did apply it, and will therefore be bound by the content and intent of the digital document that was signed by that user. This type of assurance is sometimes referred to as "non-repudiation".

Thus the grocery store can be sure that the Jones' really do want the shopping list items in their message and if included, the authorisation of a credit card payment can be accepted without doubt prior to the shopping list items being delivered. The military order to fire a missile is real and if authorised by the appropriate military commander should be carried out without question.

Digital Certificate

A further use of a digital signature is to create a certificate which is a statement by the signer about another person or fact. A certificate is usually an indication

that the issuer of the certificate confirms certain information or that it has a particular property.

In the paper domain a certificate is something which attests to a fact, like graduation from University. The certificate is typically hard to forge as it will normally have a seal that can only be applied by or with the authority of the Chancellor of the University.

In practice there are other ways of verifying that a person has graduated from a University but the certificate is typically taken at face value.

Digital signatures can also be used to uniquely sign a document which acts like a certificate. In some ways a digital certificate is better than a paper certificate since a digital certificate can be checked by an equivalent device to that of a PKPD for decrypting and checking the veracity of the private key used to create the certificate as well as displaying the document which could not have been altered while bundled with the certificate.

The term certificate is frequently used to refer to a particular type of certificate, which is used to confirm a user's "public key" the second part of an asymmetric key system where the first part is the user's "private key". Such "public key" certificates are typically created by a third party, the third party being trusted by all users to take a user's (a user known to the required level by the third party) public key and bundle it into a "public key" certificate.

Thus the second user in possession of the first user's "public key" certificate can be sure it is actually that user's public key.

The reason for this procedure is to ensure that the second user does not use what they thought was the first user's public key when in fact it is the public key of a rogue user masquerading as the first user.

In such a masquerade it is not inconceivable for the rogue user to pretend to be the first user and dependent on the relationship (eg buyer/seller; general/soldier) the consequences of the second user being deceived could be catastrophic.

Thus, since the creation of a certificate can be very critical, it is best that the process is conducted on a PKPD which is immune to "endpoint" attacks.

Referring to Fig. 1 the various means displayed may not be provided in hardware but may be virtual means and implemented in software. For example, as stated previously, the communications port 22 may be a virtual TCP/IP port having a simple physical bus connection. A further example is the cryptographic engine which could be a function of a Central Processing Unit (CPU) which interacts with both on board and external memory and peripheral hardware.

However, it is preferable that the architecture of the PKPD be as simple as possible since the less hardware and software the more it is amendable to high assurance evaluation, as may be prescribed in the various documents mentioned previously to achieve an acceptable level of trust worthiness as relevantly defined.

The function of the PKPD which requires the greatest trust is that which ensures that the users key (private, public) or the PKPD's own key, is used once and only

once; used only to sign the data which has been displayed; and is only used if the user operable input means is activated by the user.

The way in which this functionality is created and the consequent high assurance evaluation of the PKPD are steps known to those skilled in the art after having been instructed of the arrangement of the invention.

The terms trust, assurance and confidence were used to describe desirable and preferable features of the PKPD and in the art these terms are generally considered to be synonymous but others may also be used.

Devices and systems including their methodology are often complex and interrelate with each other, humans and external influences in unexpected ways. However, device and system failure is unacceptable in so called critical situations and one such failure is in the failure of security in handling digital data. Designers of so called critical systems are obliged to demonstrate that their system has been implemented in such a way that the likelihood of failure is suitably low since it is very difficult to completely eliminate the likelihood of failure in any system.

Clearly in the digital domain, failure is not only by way of failure to perform a particular function it is also the designed ability to resist the persistent attack of hostile or mischievous system users who want to take advantage of weaknesses in the system.

The more critical the system is, the lower the acceptable likelihood of failure becomes and generally the lower it becomes the more expensive the system. Furthermore, the more complex the system becomes, the harder it is to achieve

an acceptably low likelihood of failure. Also, the more complex a system is the more difficult and expensive it is to evaluate the presence or absence of faults and bugs in the implementation.

Thus, we as humans, learn to allocate different levels of trust to various systems but the meaning of the term "trust" will always be a property of the context of its use and our understanding of the likelihood of failure.

Persons skilled in the art will generally recognise the property which makes a system trusted, but in some cases it will be necessary to explicitly define the property.

Thus, in a PKPD as stated previously, it is preferable that it be trusted to use a stored key on the displayed document and only used if the user operable input means is activated. Clearly the key must be secured from unauthorised access and may if desirable be stored in encrypted form.

In the case of a public key, it must be stored so that it can not be altered in an unauthorised way.

The display means 24 as depicted in Fig. 1 and used in other embodiments described in this specification is a device for converting data into a human readable form. Display technologies are everchanging examples of which include CRT monitors and LCD monitors. Other types of display include printers and even Braille output devices so that the sight impaired can perceive the data.

It is preferable in the context of the important use of a PKPD that the monitor be trusted to display exactly the data presented to it and that the displayed form of

the document be such that the user who observes the display can not, once having signed the data with a PKPD, declare that the data was not displayed accurately to them.

Figs. 5 and 6 depicts PKPD's 40 and 50 respectively, each having their own monitors 46 and 62 and further in Fig. 6 the PC's monitor 56 can be used to display exactly the data to be reviewed by the user of the PKPD.

Thus it may be that the data format is standardised in that all characters are a minimum size and predetermined font. It may also be important to filter the data to exclude all macro's or executable because it is important to be sure that only displayable data is reviewed and signed.

Importantly, it is highly preferable that only that data which is displayed is signed by the predetermined key held in safe storage in the key storage means.

The user operable input means 28 depicted functionally as a block in Fig. 1 could be in one of the various forms previously described, importantly, it will be apparent to those skilled in the art that the means itself is a typically mechanical one that requires interaction of the human user and thus not operable by a rogue program. This means that the signal generated by the switch is not capable of being replicated by any equivalent signal generated even within the PKPD itself. In a highly critical environment where a PC and keyboard can not be trusted. This clearly obviates the use of a software equivalent or any combination of keyboard based keys associated with the user's PC.

It is also clear that there is preferably a degree of physical security related to the PKPD and the times at which it is being used by the user. The PKPD may

preferably require the user to identify and authenticate to the PKPD before it functions as required. Such identification and authentication may involve the use of user id, password, pass phrase, PIN, token, biometric or other means, or combinations thereof.

In this regard, it is possible as will be described in other aspects of the invention that the key storage means is physically removable from the PKPD and although the keys are stored therein they can not be physically extracted, otherwise any attempt to do so will destroy the keys and possibly the removable memory device itself.

Furthermore, the operation of the PKPD can be predicated on the successful response to a challenge to the proper user by the PKPD. The challenge could be in the form of a question and a predetermined response by the user. The answer could require a further input to the PKPD in the form of a keyboard for example providing numeric or alpha numeric input for the response or a biometric response in the form for example of a iris check by an appropriate sensor device included in the PKPD device (not shown).

In addition to the physical requirement to operate the PKPD (eg insertion of a valid key storage means (eg SMART CARD or FORTEZZA CRYPTO CARD)) and a valid challenge response, it may also be preferable to operate an audit log of all transactions performed or attempted with the device.

An audit log comprises a collection, typically strictly chronological, of information representative of all transactions performed by the PKPD. Such a log will identify (typically after the fact) those transactions which should not have

taken place and thus unauthorised use of the signature by even the authorised user will be available for scrutiny.

Preferably security properties of an audit log include the inability to alter or clear the log and with this property intact it is possible to claim non-repudiation of the transactions in respect of the user performing the transaction.

Although, the PKPD has been described and likely understood to be useable by only one user, it is possible for a PKPD to be useable by multiple users as long as it can partition the separate user's keys or alternatively accept multiple insertable key storage means.

Fig. 2 depicts a further embodiment of the invention of a PKPD comprising similarly identified elements such as a communications port 22, a display 24, a user operable input means (accept key) 28 but elements such as a cryptographic engine (30 in Fig. 1) are replaced or enhanced by the use of a CPU 30a, a RAM 30b and a ROM 30c.

Additional elements comprise a smartcard interface 32 for the insertion of a smartcard containing a specific user's keys, and a video switch 34 for receiving a video signal from an attached PC, and passing that signal to the PC's monitor, except when the PKPD is active, in which case the PKPD's display information is passed to the monitor. Such an arrangement is depicted in Fig. 6 where the PKPD 50 is located physically between the user's PC 52 and its monitor 56, keyboard 54 and pointing device 48.

If the PKPD uses the PC's monitor for display of information to the user, it is preferable to have an additional unforgeable indicator which can be used to

inform the user whether the information displayed on the monitor is trusted (coming from the PKPD) or not (coming from the PC). An example of such an indicator may be a LED on the PKPD front panel, near the user operable input means 64 on Fig. 6.

There is also a Private Key Storage means 38 for the PKPD's own private key the use of which will be discussed later in the specification.

The video switch 34 of this embodiment is arranged to take over control of the user's own PC monitor and replicate the trusted display function described previously. Thus even if this embodiment did not have a display 24, it could still display the received data/document in a trusted manner on the user's PC monitor. Also refer to Fig. 6 for a depiction of such an arrangement.

The smart card reader 32 allows the PKPD to have a further level of security since the smart card containing the user's keys and other selected keys can be kept in a physically secure place until it is needed saving the need to physically secure the whole PKPD which invariably would have involved disconnecting and storing a more bulky device than a smart card if connected with cables (wireless PKPD's are also possible).

Furthermore as stated previously, multiple users can use the same PKPD.

Yet further this embodiment has the provisions to apply a signature unique to the PKPD itself. This provides further surety to the recipient that the user's signature was indeed created on a PKPD, and not on, say, an untrusted PC. This could indicate to the recipient that the originator was willing to be legally bound by the message, and that the originator would not be able to repudiate having

sent the message. (Contrast this with a message without the PKPD signature: the originator could establish reasonable doubt about the fact that he deliberately signed the information, by proposing the plausible scenario in which a virus or Trojan horse on his PC signs information with his signature, without his knowledge). The existence of a PKPD signature assures the recipient that a PKPD was used by the originator and furthermore increases the non repudiation factor of the originator.

The PKPD could be constructed in such a way as to interpret organisational policy before permitting information to be signed with an organisation's signature. For example, it may be that the PKPD will only sign a message with a company's private key (which is stored inside the PKPD) if at least two of the company's directors have individually signed the message.

A certificate issuer could use a PKPD to create certificates. The certificates could be signed twice, once using the issuer's personal private key, and the second time using the PKPD private key. Any person wishing to rely on such a certificate in the future could have greater confidence in the fact that the issuer deliberately intended the certificate to be signed, because of the presence of the PKPD signature. In contrast, if the issuer's PC was infiltrated by malicious software, that software could create any certificates it wanted, and if the issuer's private key were available to the PC (either directly, or via a smartcard or Fortezza card), the certificate could be signed with that key without the issuer's knowledge or consent.

Fig. 3 depicts a message text (document) which has been first signed by User B's public key (ie can only be decrypted (unbundled) by User B's private key) and the signed document is then signed again by the User B's PKPD public key (ie

the result can only be decrypted (unbundled) by a corresponding PKPD private key).

This arrangement provides a message which can only be decrypted with both the private key of User B and the private key of User B's PKPD. It would be possible to construct the PKPD to display the decrypted version of such messages to User B, but to ensure that the decrypted version was never released outside the PKPD. This would mean that although User B could view the decrypted information on his screen, he wouldn't be able to print it, save it on disk, or forward it to any other user. Such a property can be referred to as an "Eyes Only" property.

An improvement in this mechanism would be to use a PKPD shared key, instead of the User B PKPD's public key to perform the second encryption. This would allow a mobile User B to read the message at any convenient PKPD, rather than at only the specific one whose public key was used.

Fig. 4 depicts the same User B public key use so that the inner layer can only be read by User B but the outer layer is signed by the PKPD's shared key so that any PKPD can remove the outer layer.

In this example a Shared Key is used, meaning that the encryption which forms part of the signature process uses a single symmetric key held by every PKPD and thus only PKPD's having that shared key may remove the outer layer.

Outer and inner layers are akin to the inner and outer envelopes of the SAFE HANDS document protocol in the paper domain.

In a further embodiment there exists a mechanism for receiving the document/message from a computer, and transmitting the signed document to its next destination directly from the PKPD via its communications port using a physical layer transport mechanism such as Ethernet, serial, parallel, PCI, SBUS, SCSI, VSB etc. Thus this mechanism excludes the transmitted signed document travelling back to the computer from which it was received.

In a yet further embodiment of the PKPD it would not only perform a signature generation function but also be capable of validating signed documents received.

The process of validating a digital signature is subject to endpoint attack. For example, a malicious e-mail program could inform the user that the signature attached to a message was valid, when this was not the case. In fact, a malicious e-mail program could display to the user any message it wanted to, as well as asserting that the message was signed in a most trustworthy way, even though no such message had ever been signed or sent.

A PKPD can be used to counter such endpoint attacks. The process of validating a digital signature involves the use of a public key. The PKPD, on being presented with a signed message, can calculate the validity of the message with respect to the public key, and then display the message contents and the signature validity to the user.

In general, a PKPD would not be configured with a public key for every potential originator. Instead, a certificate hierarchy is likely to be used, involving a single "root" certificate (typically self-signed), from which other certificates can be validated, eventually assuring the relationship between the originator and the originator's public key. The PKPD, on being presented with a signed message for

validation, as well as the appropriate chain of certificates (typically retrieved from a directory) can calculate the validity of the certificate chain, as well as the validity of the message. The contents of the message and signature validity, as well as the certificate chain details, can be displayed to the user.

The protection of the root certificate is important. An attacker who could modify the root certificate could supply a complete chain of "bogus" certificates, which would be valid with respect to the modified root certificate. Current e-mail programs are vulnerable to this threat. A PKPD would have to store the root public key in a manner which would prevent its unauthorised modification. Physical and procedural means could be used to provide this security.

A yet further embodiment of the use of a PKPD is to incorporate into the message being signed an "indicator" which can act as a flag to network security devices that there is an authentically signed message within the outer layer/s. The network security devices then may allow the signed document to leave, let us say a high security network for a network of lower security. This "indicator" can indicate that the message has been sealed and that it is safe for the message to be transported via insecure communication means (eg the Internet) to its intended destination. It is thus possible to implement a multi-level secure (MLS) messaging system. Fig. 7 is an illustration of various PC's and associated PKPD's communicating via local and Internet networks.

In another embodiment the PKPD would be programmed to produce signatures using standard protocols, such as MSP, CSP (ACF-120), S/MIME, PGP, etc.. This would have the advantage that commercial off the shelf infrastructure used elsewhere would "understand" the signature, although it may not fully appreciate the high assurance nature of such signatures.

In some protocols, such as MSP, CSP, S/MIME, where there can be two signatures, the device can offer advantages over those mentioned above. The PKPD can create one signature using the user's private keys, which may be used for purposes unrelated to the devices' invention. A second signature can be created using special keys devoted solely to the function of the PKPD.

A user may have private keys which are used for a variety of functions apart from the ones described in this document. For example, keys may be used for the authentication and establishment of a remote login session over the Internet. Another embodiment of the PKPD could accept requests from the connected PC that would ordinarily have been dealt with by a smartcard or Fortezza card connected directly to that PC. The PKPD would preferably alert the user to the fact that the keys were being used (although it would not necessarily be able to indicate to the user for exactly what purpose they were being used), before performing the appropriate signature, validation, encryption, or decryption (or other) operation. Although such a system would potentially allow the user's key to be abused by malicious software, the PKPD's own private key would not be made available in the same way. Its use would be reserved for instances in which the user is able to make an informed, deliberate, and legally binding choice to sign the document after it has been displayed by the PKPD.

A PKPD will be able to create a second signature, using special keys, to indicate the high assurance nature of the signature. Preferably, the user's keys would be used to create an inner signature, which would be encompassed by the second signature created by, for example the Fortezza Crypto card, using the PKPD's private key.

A signature validating device being a slight variant of a PKPD can thus translate the twice signed document into a conventional document while providing the necessary assurance of its originator and the particular PKPD which applied the signatures.

In large financial institutions, it is not practical to have "manually" signed cheques. Instead, the signatures are printed (by machine) onto the cheques. If it were possible for malicious software to be introduced into such a system, cheques could be obtained improperly. It would be possible to use PKPDs to secure the cheque printing process. An authorised user would have to review the appropriate details for the cheques, and then "accept" them on the PKPD, which would sign a message containing the details. Another PKPD, connected directly to the cheque printer, would verify that every order to print a cheque had been signed by a PKPD. Since the graphic containing the authorising (printed) signature is stored only within this latter PKPD, it would not be possible to print illegitimate cheques without using the PKPD. This would counter the threat of malicious software. The printer will need to be connected directly to the PKPD. Since the graphic containing the authorising (printed) signature is stored only within the PKPD, cheques appearing with the particular graphic could only have been produced with a high assurance PKPD. Such a signature would be unique to the printed content of the cheque (be that the amount, the words describing the amount, the date, the time, the payee and a unique transaction number).

The PKPD could be programmed to display information in particular formats which are in a convenient human readable form. For example, if messages are written in Hyper Text Markup Language (HTML), the device could render the HTML, instead of showing all of the tags of the generated signature within the message.

High value electronic transactions may be required to be authorised using a high assurance PKPD and to facilitate easier transactions, the PKPD monitor would display Secure Electronic Transaction (SET) messages in a form convenient to the PKPD user.

The device of the invention is preferably able to check the authority of the user to sign certain types (eg. classifications) of messages, before proceeding to allow a user to do so. The user's authority could be stored with the keys, or in certificates communicated to the device with the message or at any other time.

The device of the invention is preferably able to encrypt information being transmitted, in order to preserve the confidentiality of the message content until it is decrypted by the recipient.

High assurance digital signature device

A preferred embodiment of the high assurance digital signature device comprises an embedded microprocessor which executes a program stored in ROM. Preferably the ROM and microprocessor are mounted on the same integrated circuit chip and arranged so that elements within the circuit cannot be changed so that the integrity of the device as created can not be interfered with.

Interfaces

In a preferred embodiment there are three operational interfaces:

Network Interface

In one embodiment the device contains an Ethernet network interface, and communications with the user's personal computer occurs over the Ethernet.

The choice of this network protocol allows the device to be used with a wide variety of personal computers, work-stations, X-terminals, and other networked computers.

In some environments, it may be possible to assume that all user's computers will have, for example, SCSI or bi-directional parallel interfaces. There is also no reason that these could not be used for communication with the device.

User Interface

In a further embodiment interfaces to the user may be categorised as **bulk inputs** or **outputs** or **Boolean inputs** or **outputs**.

1. A Boolean output interface could be as simple as a light emitting diode (l.e.d.) Such an output only needs to indicate whether the bulk output interface is active or not. When the l.e.d. is lit, it may indicate that the device has taken over the user's screen as described in a previous embodiment.
2. The preferred bulk input interface is the keyboard of the user's computer. In other trusted systems a keyboard switch has been used to divert the output data from the keyboard to a different destination. Similar technology is used in this embodiment to divert the representations of keystrokes on the keyboard or other input device to the PKPD, instead of the user's computer. An alternative mechanism is to have a keypad or keyboard built into the PKPD. A bulk input device is used for the entry of data, such as, personal identification (PIN) phrases etc.
3. The preferred bulk output interface is the monitor of the user's personal computer. Just as the keyboard switch described above is used to "takeover" the

keyboard, a video switch is preferably used to allow the device to "takeover" the monitor. Any output displayed on the monitor by the device can be trusted to be the output provided from the bulk input interface. The user can tell whether the information on the monitor is that supplied from the device or not, by checking the status of the Boolean output which, for example, may be a light emitting diode (l.e.d.). A monitor may also be built into the PKPD. Figs 5 and 6 display these two arrangements. The PKPD 40 in Fig 5 is merely connected to the users PC 42 communication port and has its own screen 46 and a user input means 44.

4. A preferred Boolean input device is a simple push button switch mounted on the device. With such a switch, the user can provide a positive indication to the device that the document being displayed on the bulk output interface is acceptable. This switch is referred to previously as a user operable input means.

User's Fortezza Crypto card Interface

In one embodiment the user is able to insert their Fortezza Crypto card into the device. This allows the PKPD to authenticate the user, by checking that the user has entered the correct PIN phrase for the Fortezza Crypto card, and it also provides a convenient secure storage for the user's private keys used for encrypting messages if need be.

Functions of the PKPD

In one embodiment the PKPD can be arranged to provide a limited range of functions. Using the "client - server" model, the PKPD can be described as a server. Note that this does not imply that it is a large machine, located in a special room, and shared by many users at once. In this embodiment it means that the PKPD does not initiate actions itself, it only responds to requests from

another system or device, which is for the purposes at hand referred to as a client.

The client, typically a user's personal computer, sends requests to the PKPD. After performing the appropriate function as determined by the request, the PKPD sends a reply back to the client.

In a preferred embodiment a number of functions which could be offered by such a device include login; set personality; submission and delivery.

An important aspect of the submit function is the secure manner of reviewing and signing operations conducted by the PKPD. The PKPD is arranged to make it impossible for the message to be modified between the reviewing and signing steps of the process but this does not imply that after reviewing the message the signing function must occur.

Secure Messaging

The following is a description of an embodiment of the way in which a high assurance digital signature device and method of use can be integrated into an existing messaging system which uses the MSP (Message Security Protocol) and a Fortezza Crypto card. A similar approach could be used for systems using other protocols.

Existing system

The typical messaging system incorporating MSP performs the login and message submission processes as follows which is in accordance with MSP ICD. Note that although the order of some steps is important, the precise order described herein is not the only valid process.

1. The user starts a Messaging User Agent (MUA) program, such as Netscape, Exchange, or Notes. As part of the start-up sequence, the user is required to login to the Fortezza Crypto card. The MUA program provides a pop up box, into which the user is asked to enter a PIN phrase. The PIN phrase is passed as an argument to the MSP_LOGIN call.
2. The MSP_LOGIN function passes the PIN Phrase to the Fortezza Crypto card, which verifies it, thus authenticating the user.
3. The MSP_LOGIN function instructs the Fortezza to provide a list of personalities, whose private keys are stored on the card.
4. The MSP_LOGIN function returns, passing the list of personalities as a result.
5. The MUA program displays the list of personalities to the user in another dialog box. The user is invited to select one of the personalities with whose key, messages will be signed, encrypted, or decryption.
6. The MUA program passes the selected personality as an argument to the MSP_SETPERSONALITY function.
7. The MSP_SETPERSONALITY function instructs the Fortezza Crypto card to select the appropriate private key.
8. When the user chooses to send a new message the MUA program creates a window for the new message, and the user chooses a recipient/s (either by

typing in addresses or choosing them from an address book), types in the message, and adds attachments if necessary. The user then selects the required security services: either none, sign, or sign and encrypt. When the composition is complete, the "Send" button is activated. The user's computer may or may not have control of the user's ability to attach certain files.

9. Submission access control then occurs.
10. The MUA program then begins the process of invoking none or "one or more" security options. For example, the Fortezza Crypto card is instructed by the MUA program to calculate a hash value (eg. MD5) and signature, and if appropriate, to encrypt the message. The signature and plain or encrypted message are constructed into a "Protocol Data Unit" (PDU) according to the protocol.
11. The PDU is attached to header or "envelope" information, which is then transferred to the messaging server, or Message Transfer Agent (MTA).
12. The typical delivery and verification/decrypted mechanism then follows.

Modifications to provide a high assurance mechanism

The following steps show the modifications required to change the existing system so that it can support the high assurance mechanism.

1. When the MUA is loaded, instead of loading in the standard MSP software as an integral part, software is loaded to allow the MUA to communicate with the PKPD. When the MUA calls the "MSP _ LOGIN" function, the software sends a signal to the device to indicate that the login

function should commence. The device allows the user to enter the PIN phrase through a built-in keypad (or through the computer's keyboard, if keyboard switching functionality is included).

2. The device returns a signal to the computer, including the listed personalities. The software receives the signal, and "returns" the list as the result of the MSP_LOGIN call. When the user chooses a personality, the MUA is loaded.
3. When the MUA software would normally call the MSP_SETPERSONALITY function, the appropriate parameters are instead transmitted to the PKPD. The PKPD displays the chosen personality to the user, and allows the user to verify that this is appropriate. This protects the user against the threat of malicious software choosing an inappropriate personality for messages about to be signed by the user. The "results" of the MSP_SETPERSONALITY function would be returned to the MUA.
4. When the MUA would previously have requested the card to hash and sign particular data, the function would instead be routed to the PKPD, in a similar way. The information being signed would be displayed to the user, and the user would have to indicate acceptance before the signature value was released back to the MUA. To perform this function, the PKPD may have to interpret appropriate protocol data units in order to present a human readable version of the message to the user.

A preferable high assurance digital signature mechanism provides one or more of the following features:

1. A message which is signed with a high assurance signature should not be vulnerable to Trojan horse software attacks on the computers of either the originator or receiver. That is, it is assumed that the software on all the systems have been maliciously changed to subvert the security of the computer but even those malicious changes will not affect the functions of a PKPD in its signing or verification functions.
2. Subject to the strength of the cryptographic algorithms it should be impossible to forge a high assurance signature.
3. The high assurance signature can preferably be conveyed within standard protocols, thus allowing a user with Commercial Off the Shelf (COTS) standard compliant software to receive messages from, and transmit messages to, a user using a High Assurance Digital Signature device and method.
4. The user should preferably be allowed to use their Fortezza Crypto card in an un-trusted computer for un-trusted applications.

It will be appreciated by those skilled in the art, that the invention is not restricted in its use to the particular application described and neither is the present invention restricted in its preferred embodiment with regard to the particular elements and/or features described or depicted herein. It will be appreciated that various modifications can be made without departing from the principles of the invention, therefore, the invention should be understood to include all such modifications within its scope.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A digital private key protection device, comprising
 - a digital private key storage means containing a user's digital private key;
 - a cryptographic engine;
 - a communications port for receiving digital data from an external device, and for transmitting data to said external device;
 - a display means for displaying said received digital data;
 - a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data; whereinsaid cryptographic engine is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device .
2. A digital private key protection device according to claim 1, wherein said digital key storage means contains a trusted public key and a plurality of user's public keys signed by said trusted private key; and said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of said user's public key and then decrypts said received data using said verified predetermined user's public key and causes said display to indicate whether said user's private key was used to sign said received digital data.
3. A private key protection system according to claims 1 and 2 wherein said signed digital data is a digital certificate.

4. A private key protection system according to claim 1 further comprising an audit means wherein signed data is not transmitted external of said digital private key protection device until a said encryption process is audited by said audit means.
5. A private key protection system according to claim 2 further comprising an audit means wherein signed data is not displayed until a said encryption process is audited by said audit means.
6. A private key protection system according to claim 1 wherein said digital private key protection device further comprises a private key protection device private key storage means wherein digital data signed by said private key protection device after operation of said user operable input means is further signed by said private key of said private key protection device.
7. A digital private key protection device according to claim 1 wherein said digital key storage means contains a predetermined digital private key protection device's public key; such that when said communications port receives signed digital data from an external device which may or may not have been signed by a said predetermined digital private key protection device;
said cryptographic engine decrypts said received data using said predetermined digital private key protection device's public key to verify whether said digital private key protection device's private key was used to sign said received data.
8. A digital private key protection device according to claim 7 wherein said display means indicates whether said digital private key protection device's private key was used to encrypt said received data.

9. A digital private key protection device according to claim 1 further comprising a public key storage means containing a plurality of user's public keys; and

said received digital data contains information that predetermines which user's public key is used to sign said received data that is transmitted external of said digital private key protection device to said predetermined user.

10. A digital private key protection device according to claim 1 wherein said cryptographic engine is trusted to decrypt digital data using said user's digital private key and passing decrypted digital data to said display means for display of said received digital data.

11. A digital private key protection device according to claim 10 wherein said cryptographic engine does not decrypt signed digital data unless said user operable input means is operated.

12. A digital private key protection device according to claim 10 wherein said communications port can not transmit said decrypted digital data.

13. A digital private key protection device according to claim 12 wherein said communications port can not transmit said decrypted digital data unless said user operable input means is operated.

14. A digital private key protection device according to claim 1 wherein said digital private key storage means also contains a digital shared secret symmetric key wherein said cryptographic engine is trusted to only apply said digital shared secret symmetric key to encrypt data only if said user operable input

means is operated and also trusted to communicate said signed data external of said digital private key protection device.

15. A digital private key protection device according to any preceding claim wherein said received digital data contains an instruction which determines how said encryption engine should encrypt or decrypt respectively.
16. A digital private key protection device according to any preceding claim wherein said received digital data contains an instruction which determines which protocol is used by said device to communicate encrypted or signed data external of said device.
17. A digital private key protection device according to any preceding claim wherein said display means is external to said device and controlled by said device for displaying data transmitted from said communications port.
18. A digital private key protection device according to any preceding claim wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner.
19. A digital private key protection device according to any preceding claim further comprising identification and authentication means actuated by said user in a predetermined manner.
20. A digital private key protection device according to claim 18 further comprising an audit means which audits said actuation of said user identification input means.

21. A digital private key protection device according to any preceding claim wherein said digital private key storage means is removable from said device.
22. A digital private key protection device according to any preceding claim wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said PKPD using the user's private or other keys as identified by the request, but excluding the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.
23. A digital private key protection device according to claim 22 wherein said device displays a description of said request to the user and, only if the user operates said user operable input means, does said device carry out said request.



2/4

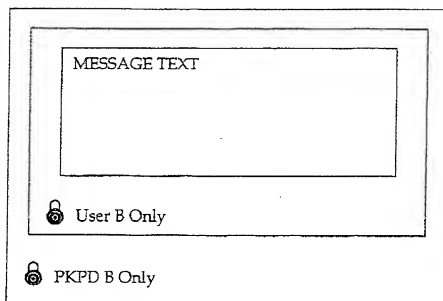


Fig. 3

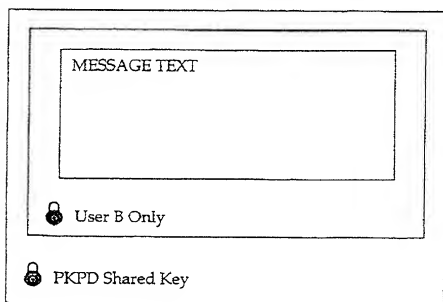


Fig. 4

3/4

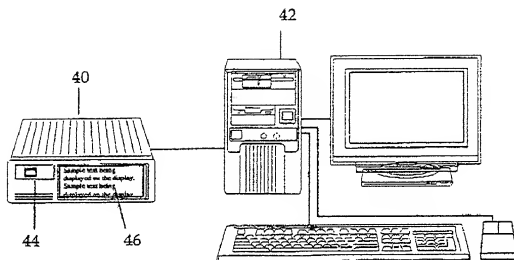


Fig. 5

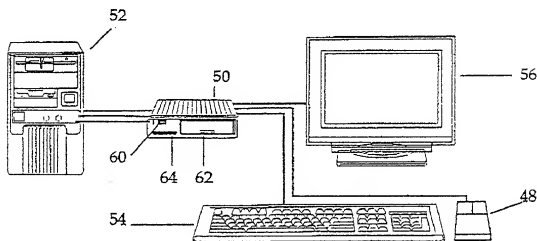


Fig. 6

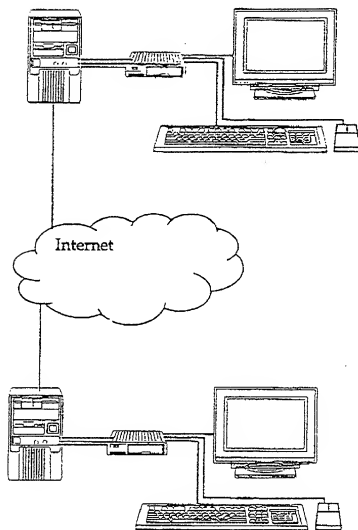


Fig. 7

COMBINED DECLARATION/POWER OF ATTORNEY

AS BELOW NAMED INVENTOR, I HEREBY DECLARE THAT: This Declaration is of the following type:

☐ Original ☐ Supplemental ☐ Continuation-In-Part
☐ Divisional ☐ Continuation ☒ National Stage of PCT

My residence, post office address and citizenship are below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: "HIGH ASSURANCE DIGITAL SIGNATURES" the specification of which:

☐ is attached hereto
☒ was filed on, as Serial No 09/856,813, received 25 May 2001
☒ was amended on (if applicable) 25 May 2001
☒ was described and claimed in PCT International Application No PCT/AU99/01051 filed on 25TH November 1999
 and was amended under PCT Article 19 on

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Sec. 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Sec.119 of the foreign application(s) for patent or inventor's certificate or of any PCT International application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America files by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Country	Appln No.	Day/Month/Year/Filed	Priority Claimed Yes No
Australia	PP 7283	25 th November 1998	YES

I hereby claim the benefit under Title 35 USC 120 of the United States application(s) listed below, and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided in the first paragraph of Title 35 USC 112, I acknowledge the duty to disclose material information as defined in Title 37 CRR 1.56(a) which occurred between the filing date of the prior application and the national or PCT International filing date of this application:

Serial No.	Filing Date	Status

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected with:

Webb Ziesenheim Logsdon Orkin & Hanson PC
700 Koppers Building
436 Seventh Avenue
PITTSBURGH PA 15219-1818
UNITED STATES OF AMERICA

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issue therefrom.

John Desborough Yesheg *[Signature]* *31/May/2001*
Full name of sole or first inventor Inventor's signature Date
44 Tuckett St, Kenmore Hills, Q. 4059 Australia
Residence *Australian*
Citizenship
PO Box 1500, Salisbury, SA, 5108, Australia
Post Office Address

Full name of second joint inventor if any Inventor's signature Date

Residence Citizenship

Post Office Address